(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 40 08 971 A 1**

(51) Int. Cl.[5]:
G 06 F 12/14
H 04 L 9/32
G 07 C 9/00

(21) Aktenzeichen: P 40 08 971.1
(22) Anmeldetag: 20. 3. 90
(43) Offenlegungstag: 26. 9. 91

DE 40 08 971 A 1

(71) Anmelder:
- Siemens Nixdorf Informationssysteme AG, 4790 Paderborn, DE

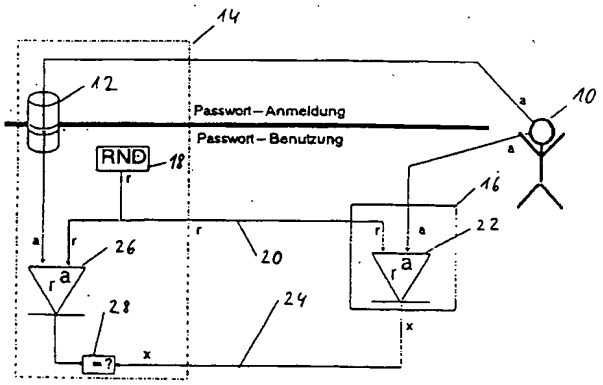
(74) Vertreter:
Schaumburg, K., Dipl.-Ing.; Thoenes, D., Dipl.-Phys. Dr.rer.nat.; Englaender, K., Dipl.-Ing., Pat.-Anwälte, 8000 München

(72) Erfinder:
Glaschick, Rainer, Dipl.-Inform., 4790 Paderborn, DE

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zur Authentifizierung eines eine Datenstation benutzenden Anwenders

(57) Bei einem Verfahren zur Authentifizierung eines eine Datenstation benutzenden Anwenders gegenüber einem mit der Datenstation verbundenen Rechnersystem, wobei im Rechnersystem mittels eines dort für den Anwender gespeicherten Paßwortes und einer im Rechnersystem erzeugten Zufallszahl ein erster Wert und in der Datenstation mittels des vom Anwender eingegebenen Paßwortes und der Zufallszahl ein zweiter Wert ermittelt und die Beziehung der beiden Werte zueinander ausgewertet wird, werden das Paßwort a und die Zufallszahl r sowohl im Rechnersystem (14) als auch in der Datenstation (16) jeweils durch eine Einwegfunktion (26, 22) verknüpft.



DE 40 08 971 A 1

Beschreibung

Die Erfindung betrifft ein Verfahren zur Authentifizierung eines eine Datenstation benutzenden Anwenders gegenüber einem mit der Datenstation verbundenen Rechnersystem, wobei im Rechnersystem mittels eines dort für den Anwender gespeicherten Paßwortes und einer im Rechnersystem erzeugten Zufallszahl ein erster Wert und in der Datenstation mittels des vom Anwender eingegebenen Paßwortes und der Zufallszahl ein zweiter Wert ermittelt und die Beziehung der beiden Werte zueinander ausgewertet wird.

Das erfindungsgemäße Verfahren befaßt sich ganz allgemein mit dem Problem der Authentifizierung bei Rechnersystemen, die jeweils mit einer Vielzahl von Datenstationen verbunden sind. Die Datenstationen können dabei Rechner mit Emulationsprogrammen, Personal Computer oder dedizierte Datenstationen sein. Sobald ein Benutzer oder Anwender auf einen Rechner über seine Datenstation zugreifen will, wird er vom Rechner aufgefordert, sich durch ein Paßwort zu authentifizieren. Er übermittelt das Paßwort an die Datenstation, die es als Nachricht zum Rechner überträgt. Das Problem besteht darin, daß ein unberechtigter Benutzer seine Datenstation so modifizieren kann, daß er eine Kopie der von der ersten Datenstation an den Rechner gesandten Nachricht empfängt und aus der Datenstation entnimmt. Danach kann sich der unberechtigte Benutzer anstelle des berechtigten authentifizieren, weil er das Paßwort kennt. Ein weiterer Mangel dieser Art der Authentifizierung liegt darin, daß ein privilegierter Benutzer, der unbeschränkten Zugriff auf die Daten im Rechner hat, sich das Paßwort eines Benutzers durch Auslesen aus dem Speicher aneignen kann.

Bei einem ersten bekannten Verfahren zur Authentifizierung wird bei der Paßwortanmeldung das unverschlüsselte Paßwort von der Datenstation des Benutzers dem Rechnersystem übermittelt. Dort wird das Paßwort mittels einer Einwegfunktion verschlüsselt und in einer Datei gespeichert. Bei der Paßwortbenutzung, d. h. bei der Authentifizierung wird dann ebenfalls das im Klartext von der Datenstation zu dem Rechnersystem gesandte Paßwort in dem Rechnersystem durch eine Einwegfunktion verschlüsselt. Als Einwegfunktion wird dabei eine Funktion bezeichnet, die einfach zu berechnen ist, für die jedoch kein Verfahren existiert, um ihre Umkehrfunktion mit vertretbarem Aufwand zu berechnen.

Der resultierende Wert wird anschließend mit dem in der Datei abgespeicherten verschlüsselten Paßwort verglichen. Bei Gleichheit gilt der Benutzer als authentifiziert. Bei diesem Verfahren ist es nicht möglich, durch Auslesen der Paßwortdatei Kenntnis von dem Paßwort zu erlangen. Allerdings kann das im Klartext an das Rechnersystem übermittelte Paßwort abgehört und anschließend mißbräuchlich genutzt werden.

Eine Verbesserung kann erreicht werden, wenn die Authentifizierung im Dialog zwischen der Datenstation und dem Rechnersystem erfolgt. Hierzu wurde bereits vorgeschlagen, ein symmetrisches Chiffrierverfahren einzusetzen. Dabei wird bei der Anmeldung das Paßwort 20 in einer geschützten Datei im Klartext gespeichert. Zur Authentifizierung wird in dem Rechnersystem in einem Zufallszahlengenerator eine Zufallszahl erzeugt, mit einer Verschlüsselungseinheit verschlüsselt und an die Datenstation geschickt. Diese Nachricht wird mit dem dem Benutzer abgeforderten Paßwort mit einem Entschlüßler entschlüsselt, durch eine Addition modifiziert, mit dem Paßwort durch den Verschlüßler verschlüsselt und an das Rechnersystem zurückgeschickt. Im Rechnersystem wird die Nachricht durch einen Entschlüßler entschlüsselt und mit der durch die Addition ebenfalls modifizierten Zufallszahl verglichen, wobei sich im Vergleicher Übereinstimmung ergeben muß. Nachteilig an dieser Lösung ist ebenfalls, daß das Paßwort einem privilegierten Benutzer (Systemverwalter) oder Anlagentechniker zugänglich ist, der die entsprechende Datei auslesen kann. Daher kann das Paßwort auch in diesem Falle gestohlen werden.

Schließlich wurde auch ein Verfahren entwickelt, das vom Benutzer die Aufbewahrung von mindestens zwei Werten verlangt. Diese Schlüssel werden von einer Schlüsselzentrale nach einem bestimmten Verfahren erzeugt und sind daher vom Benutzer nicht frei wählbar, so daß dieser nicht ein mnemotechnisches Paßwort wie in herkömmlichen Paßwortlösungen selbst wählen kann. Da sich der Benutzer aus Sicherheitsgründen das Paßwort nicht aufschreiben darf, ist das Verfahren nur in Verbindung mit Chipkarten praktikabel.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren der eingangs genannten Art anzugeben, das eine höhere Sicherheit bei einfacher Handhabung bietet.

Diese Aufgabe wird bei einem Verfahren der eingangs genannten Art dadurch gelöst, daß das Paßwort und die Zufallszahl sowohl im Rechnersystem als auch in der Datenstation jeweils durch eine Einwegfunktion miteinander verknüpft werden. In diesem Falle wird das Paßwort niemals im Klartext über eine der Verbindungsleitungen zwischen der Datenstation und dem Rechnersystem gesandt. Es kann daher auch nicht abgehört und mißbräuchlich benutzt werden. Dabei kann das Paßwort bei der Anmeldung über einen geschützten Kanal, beispielsweise durch einen Boten, dem Rechnersystem mitgeteilt und im Klartext gespeichert werden, wobei diese Lösung allerdings noch den oben genannten Nachteil hat, daß die Datei durch einen privilegierten Benutzer oder Anlagentechniker ausgelesen werden kann. In diesem Falle ist es zweckmäßig, bei der Paßwortanmeldung dieses bereits durch eine Einwegfunktion zu verschlüsseln und im verschlüsselten Zustand zu speichern.

Eine erhöhte Sicherheit erhält man auch, wenn die Zufallszahl vor ihrer Übermittlung an die Datenstation durch eine Einwegfunktion verschlüsselt wird. Um unter den vorstehend beschriebenen Voraussetzungen auf einfache Weise im Rechnersystem und in der Datenstation Werte zu erzeugen, die miteinander verglichen werden können, ist es zweckmäßig, zur Verschlüsselung des Paßwortes und zur Verknüpfung des verschlüsselten Wertes mit der Zufallszahl in dem Rechnersystem einerseits und zur Verschlüsselung der Zufallszahl und ihrer Verknüpfung mit dem verschlüsselten Paßwort in der Datenstation andererseits kommutative Einwegfunktionen zu verwenden, wie dies weiter unten noch näher erläutert wird.

Die Verknüpfungs- und/oder Verschlüsselungsschritte mittels Einwegfunktionen können auch mindestens einmal wiederholt werden.

Um gegen die Vortäuschung eines Rechnersystems (anstelle des tatsächlich vorhandenen Rechnersystems) gesichert zu sein, kann das Verfahren auf gegenseitige Authentifikation erweitert werden, in dem die verschiedenen Verfahrensschritte in dem Rechnersystem und der Datenstation verschachtelt gleichzeitig ablaufen.

Es besteht auch die Möglichkeit, den durch Verschlüsselung des Paßwortes bei der Anmeldung erzeugten

Wert, den sogenannten Authentifikator, nicht in dem Rechnersystem abzuspeichern, sondern ihn dem Rechnersystem zusammen mit der Identifikation zu übermitteln, wobei der Authentifikator durch ein Signaturverfahren an sich bekannter Art beglaubigt ist. Damit wird jeder Versuch unterbunden, durch Auslesen der entsprechenden Datei in dem Rechnersystem an den Authentifikator und damit unter Umständen doch noch an das Paßwort zu gelangen.

Die Operationen mit den Schlüsselfunktionen können in einer versiegelten Einheit stattfinden, in der sich der geheime Schlüssel befindet und nicht ausgelesen werden kann. Lediglich der Authentifikator ist in diesem Falle elektronisch oder optisch lesbar. Eine solche Einheit kann beispielsweise als Chipkarte ausgebildet sein.

Als Einwegfunktion kann beispielsweise die diskrete Exponentiation modulo einer ganzen Zahl oder einer Polynomerweiterung eines Zahlenringes verwendet werden.

Die mathematischen Grundlagen hierfür sind an sich bekannt. Dabei werden die Berechnungen modulo einer großen Primzahl q ausgeführt, so daß nur die Zahlen von 0 bis ausschließlich dieser großen Zahl q auftreten. Zu diesem Modul wird eine weitere Zahl w bestimmt, die ein primitives Element des Galois-Körpers GF (q) ist. Dies bedeutet, daß die Potenzen w^i von w alle verschieden sind, solange i kleiner als q ist. Da q eine Primzahl ist, ist jede Zahl $w < q$ ein primitives Element.

Alternativ hierzu können auch die Rechenverfahren der Polynom-Arithmetik angewendet werden modulo zu einem irreduziblen Polynom vom Grade n. Vor- und Nachteile sind ausreichend in der Literatur besprochen und nicht Gegenstand der vorliegenden Erfindung.

Unter diesen Randbedingungen ist die Funktion $f(x, y) = x^y$ einfach zu berechnen, aber die inverse Funktion $f^{-1}(x, z) = \log_x z$ ist nur mit sehr großem Rechenaufwand berechenbar. Für q ungefähr 2^{200} benötigt die Exponentiation ca. 200 Multiplikationen (von 200-Bit-Werten). Die besten bekannten Verfahren zur Logarithmusbildung jedoch benötigen 10^9 Multiplikationen. Damit ist die Eigenschaft einer Einwegfunktion gegen. Wegen

$$f(f(x,y),z) = (x^y)^z = x^{(y*z)} = (x^z)^y = f(f(x,z),y)$$

ist die Exponentiation rechts-kommutativ.

Die folgende Beschreibung erläutert in Verbindung mit den beigefügten Zeichnungen die Erfindung anhand von Ausführungsbeispielen. Es zeigen:

Fig. 1 ein Ablaufschema des erfindungsgemäßen Verfahrens gemäß einer ersten Ausführungsform und

Fig. 2 ein Ablaufschema des erfindungsgemäßen Verfahrens gemäß einer zweiten Ausführungsform.

Das in der **Fig.** 1 dargestellte Verfahren soll das Abhören des Paßwortes bei der Authentifizierung verhindern. Es wird dabei zwischen der Paßwortanmeldung, einem einmaligen Vorgang, und der Paßwortbenutzung oder Authentifizierung, einem beliebig wiederholbaren Vorgang, unterschieden. Bei der Paßwortanmeldung wird das vom Benutzer **10** gewählte Paßwort a über einen geschützten Kanal, z. B. durch einen Boten, in eine geheime Datei **12** eines Rechners **14** eingetragen und dort im Klartext gespeichert. Will der Benutzer anschließend eine Leistung des Rechners **14** über eine mit diesem verbundene Datenstation **16** abrufen, so wird seine Berechtigung hierzu überprüft (Authentifizierung). Dies erfolgt in der Weise, daß in einem Zufallsgenerator **18** eine Zufallszahl r gebildet wird, indem beispielsweise die Tageszeit mit der Prozeßnummer multipliziert wird. Diese Zufallszahl r wird über einen Kanal **20** zur Datenstation **16** übertragen. In der Datenstation wird nach Anforderung des Paßwortes a in dem Funktionsrechner **22** die zweistellige Einwegfunktion "modulare Exponentiation" ausgeführt, indem der Wert $x = r^a$ gebildet wird. Dieser Wert x wird über einen Kanal **24** an den Rechner **14** zurückübertragen. Im Rechner **14** wird zeitgleich mit den Vorgängen in der Datenstation **16** unter Verwendung des in der Datei **12** gespeicherten Paßwortes a und der Zufallszahl r in einem Funktionsrechner **26** ebenfalls der Wert r^a gebildet. Dieser Wert und der Wert x werden in einem Vergleicher **28** miteinander verglichen. Bei Gleichheit gilt der Benutzer als authentifiziert. Aus den über die Kanäle **20** und **24** übertragenen Daten kann das Paßwort wegen der Einwegeigenschaft der modularen Exponentiation nicht mit vertretbarem Aufwand ermittelt werden. Damit kann das Paßwort a auch nicht durch Abhören der Verbindung zwischen der Datenstation **16** und dem Rechner **14** ermittelt werden. Allerdings ist das Paßwort im Rechner **14** für einen privilegierten Benutzer zugänglich gespeichert.

Um auch diese Mißbrauchsquelle zu verstopfen, wurde das Verfahren gemäß Abbildung **2** erweitert. Gleiche Teile sind wiederum mit gleichen Bezugsziffern versehen. Im Gegensatz zu der Lösung gemäß **Fig.** 1 wird das Paßwort bei der Paßwortanmeldung in der Datenstation **16** mittels eines Funktionsrechners **30** durch eine Einwegfunktion verschlüsselt, indem der Authentifikationswert $u = w^a$ berechnet wird. Dieser Authentifikationswert u, der das Paßwort a nur in einer verschlüsselten Form enthält, wird dem Rechner **14** zugeführt und in der Datei **12** gespeichert.

Ferner wird bei der Authentifizierung die Zufallszahl r vor dem Übermitteln an die Datenstation **16** in einem Funktionsrechner **32** verschlüsselt, indem der Wert $x = w^r$ berechnet wird. Dieser verschlüsselte Wert x wird über den Kanal **20** der Datenstation **16** zugeführt.

Bei der Authentifizierung wird dann in dem Funktionsrechner **26** des Rechners **14** der Wert $z = u^r = w^{a*r}$ gebildet. In dem Funktionsrechner **22** der Datenstation **16** wird der Wert $y = x^a = w^{r*a} = w^{a*r}$ gebildet. Man erkennt, daß trotz des unterschiedlichen Berechnungsweges die Funktionen z und y identisch sind. Bei Gleichheit der Wert y und z gilt der Benutzer **10** wieder als authentifiziert. Bei dem Verfahren gemäß Abbildung **2** ist es weder während der Paßwortanmeldung noch während der Paßwortbenutzung möglich, durch Abhören der Kanäle zwischen der Datenstation **16** und dem Rechner **14** das Paßwort a zu ermitteln. Auch die Kenntnis des Inhaltes der Datei **12** führt nicht zur Kenntnis des Paßwortes a. Der Authentifikator u und der Wert w können bekannt sein. Dennoch ist es nicht möglich, mit vernünftigem Aufwand das Paßwort a zu ermitteln.

Die Berechnungen der Datenstation können vollständig in einer Chipkarte realisiert werden, so daß der Benutzer sein Paßwort nicht einer Maschine anvertrauen muß, auf die er keinen Einfluß hat und die manipuliert sein könnte.

Um gegen die Vortäuschung eines Rechnersystems gesichert zu sein, kann das Verfahren leicht auf gegenseitige Authentifizierung erweitert werden, indem die beiden Verfahren gleichzeitig ablaufen und die jeweiligen Nachrichtenblöcke die Informationen beider Verfahren tragen. Die Anzahl der Kommunikationsschritte zwischen dem Rechner und der Datenstation erhöht sich dadurch nicht.

Die Lösung gemäß **Fig.** 2 kann noch dadurch erweitert werden, daß im Rechensystem $k_s = p^r = w^{s*r}$ und in der Datenstation $k_s = x^s = w^{r*s}$ gebildet werden. Beide Werte sind gleich, wie bereits oben festgestellt wurde. Sie können jedoch nicht durch Belauschen der Datenverbindungen ermittelt werden. Sie sind daher als "session-keys" für die Verschlüsselung der nachfolgenden Datenkommunikation mit einem symmetrischen Verfahren geeignet.

Anstelle der Vorbereitung, in der über einen authentifizierten Kanal der Authentifikator vom Anwender zum Rechner übermittelt und dann vom Rechner gespeichert wird, kann auch das Paar (Anwender, Paßwort) mit einer digitalen Unterschrift versehen werden, wie dies beispielsweise in El-Gamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE-IT 31 (1985), Seiten 469–472 beschrieben ist. Bei der Identifikation schickt dann der Anwender zusammen mit seinem Namen A auch das zertifizierte Paket A, a. Diese Variante ist nützlich, wenn ein Anwender mit mehreren verschiedenen Rechensystemen kommuniziert. Dann wird der Authentifikator durch eine Zulassungsstelle versiegelt.

Patentansprüche

1. Verfahren zur Authentifizierung eines eine Datenstation benutzenden Anwenders gegenüber einem mit der Datenstation verbundenen Rechnersystem, wobei im Rechnersystem mittels eines dort für den Anwender gespeicherten Paßwortes und einer im Rechnersystem erzeugten Zufallszahl ein erster Wert und in der Datenstation mittels des vom Anwender eingegebenen Paßwortes und der Zufallszahl ein zweiter Wert ermittelt und die Beziehung der beiden Werte zueinander ausgewertet wird, **dadurch gekennzeichnet,** daß das Paßwort a und die Zufallszahl r sowohl im Rechnersystem (14) als auch in der Datenstation (16) jeweils durch eine Einwegfunktion (26, 22) verknüpft werden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß das Paßwort a vor seiner Übermittlung an das und seiner Speicherung in dem Rechnersystem (14) durch eine Einwegfunktion (30) verschlüsselt wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Zufallszahl r vor ihrer Übermittlung an die Datenstation (16) durch eine Einwegfunktion (32) verschlüsselt wird.

4. Verfahren nach den Ansprüchen 2 und 3, dadurch gekennzeichnet, daß zur Verschlüsselung des Paßwortes a und zur Verknüpfung des verschlüsselten Wertes u mit der Zufallszahl einerseits und zur Verschlüsselung der Zufallszahl r und ihrer Verknüpfung mit dem unverschlüsselten Paßwort a andererseits kommutative Einwegfunktionen verwendet werden.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß die Verknüpfungs- und/oder Verschlüsselungsschritte mittels Einwegfunktionen mindestens einmal wiederholt werden.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß als Einwegfunktion die diskrete Exponentiation modulo einer ganzen Zahl oder einer Polynomerweiterung eines Zahlenringes verwendet wird.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, eine gegenseitige Authentifizierung von Anwender und Rechnersystem nach einem der Ansprüche 1 bis 6 erfolgt, wobei die verschiedenen Verfahrensschritte verschachtelt gleichzeitig ablaufen.

8. Verfahren nach einem der Ansprüche 2 bis 7, dadurch gekennzeichnet, daß der Authentifikator dem Rechner vom Anwender zusammen mit der Identifikation übermittelt wird, wobei der Authentifikator durch ein Signaturverfahren beglaubigt wird.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß die Verschlüsselungsvorgänge in einer versiegelten Einheit (Chipkarte) stattfinden, in der sich der geheime Schlüssel (Paßwort) nicht-auslesbar befindet, wobei lediglich der Authentifikator elektronisch oder optisch lesbar ist.

Hierzu 2 Seite(n) Zeichnungen

Nummer: DE 40 08 971 A1
Int. Cl.[5]: G 06 F 12/14
Offenlegungstag: 26. September 1991

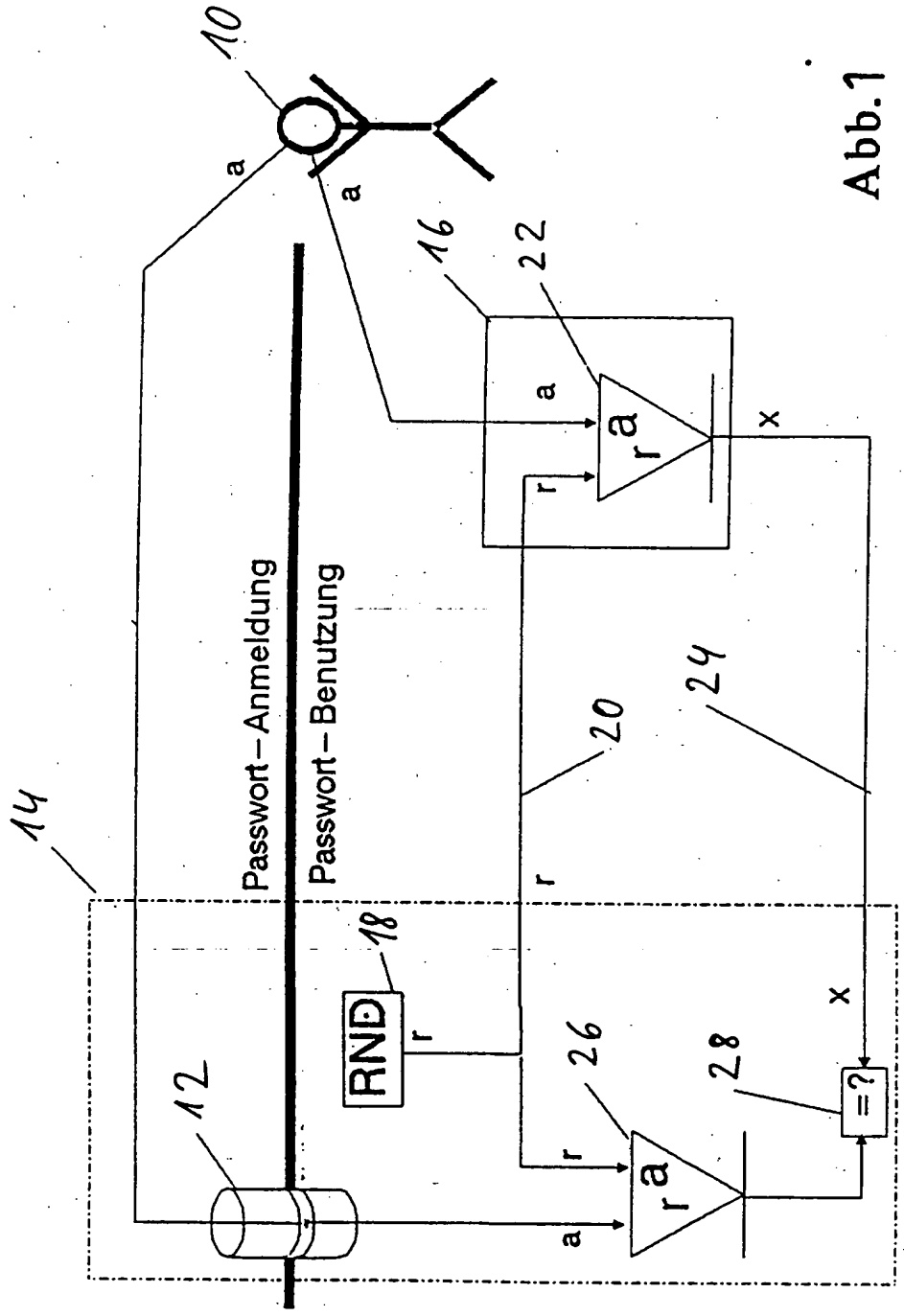


Abb.1

Nummer: DE 40 08 971 A1
Int. Cl.[5]: G 06 F 12/14
Offenlegungstag: 26. September 1991

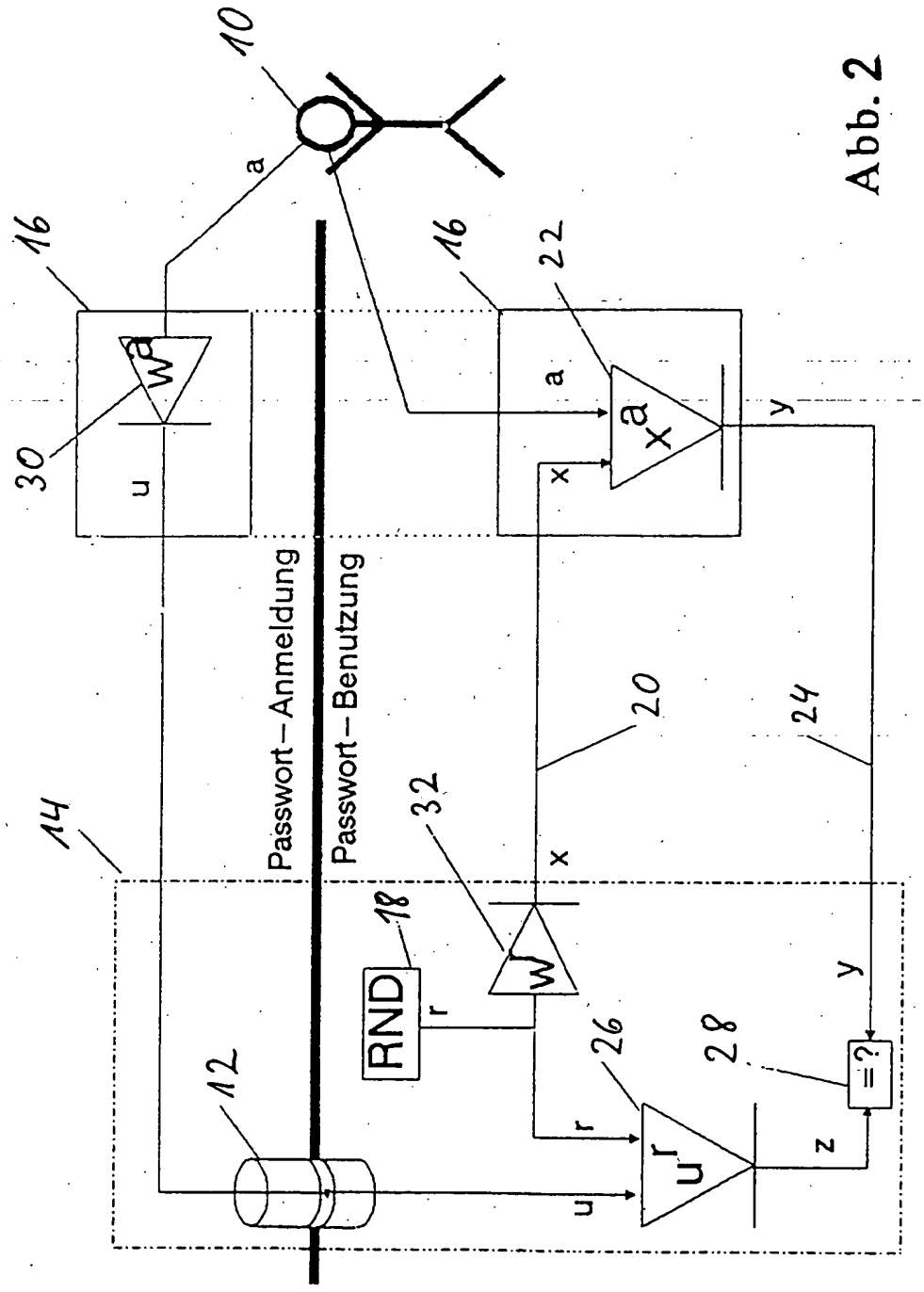


Abb. 2